Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

[redacted]

21 October 1985

NOTE FOR: C/OLL/CIA

FROM: [redacted] STAT
Chief, Legislative Liaison

SUBJECT: Materials from SSCI Staff Pertinent to Upcoming Hearings on Counterintelligence

1. Attached are two documents that I received today from Ed Levine and John Elliff of the SSCI Staff. Attachment A is a copy of the joint statement that Senators Durenberger and Leahy plan to make before the Senate Permanent Subcommittee on Investigations hearing tommorrow on "Espionage Activities in the United States".

2. Attachment B is the "briefing book outline" that the SSCI staff will put in their members notebooks for the SSCI's five upcoming hearings on security and counterintelligence. This outline reflects the staff's thinking on how the SSCI hearings will be structured, from a topical standpoint.

[redacted] 5

3. They are offering these materials as an aid to the DCI in preparing for the Committee's upcoming hearings.

[redacted] STAT

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0
ATTACHMENT A

STATEMENT OF

SENATOR DAVE DURENBERGER, CHAIRMAN
SENATOR PATRICK LEAHY, VICE CHAIRMAN

SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

BEFORE THE

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
COMMITTEE ON GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

October 22, 1985

FOR RELEASE ON DELIVERY
Expected at 9:30 a.m.
Tuesday, October 22, 1985

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

We appreciate the opportunity to testify before the Permanent Subcommittee on Investigations with regard to the hostile intelligence services threat and the actions required to counter that threat. The Subcommittee has done outstanding work on security issues. The hearings in 1982 on Soviet efforts to acquire American technology helped make the public and the Congress aware of the seriousness of the problem. The hearings on personnel security last spring demonstrated the need for major improvements in security clearance policies. The Select Committee on Intelligence is committed to following up on the recommendations that emerged from those hearings.

We are especially pleased that today's hearing will focus on ways to control the numbers and activities of Soviet and other foreign representatives who conduct espionage and related activities in the United States. The Soviet bloc presence goes far beyond their diplomats in Washington and amounts to some 2,500 positions in embassies, U.N. Missions, the U.N. Secretariat, trade and commercial operations and other offices. Much more must be done to counter the intelligence threat posed by these potential and actual intelligence agents.

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Several cases show why the problem goes beyond just Soviet diplomats. In 1983, an employee of the Bulgarian trade office in New York -- a man named Kostadinov -- was arrested for espionage based on evidence that he bought a secret document on security procedures for American nuclear weapons. Kostadinov had been working in the trade office without diplomatic immunity since 1979. A second case involved an American businessman, James Harper, who sold documents from a defense contractor's office on Minute-man missile secrets to Polish intelligence. The key figure who introduced Harper to the Poles was another California businessman, William B. Hugle, whose firm had received large payments from the Polish electronics firm Unitra. The use of commercial cover and business dealings for espionage purposes is documented in other cases, including the Bell case where an employee of a defense contractor was recruited as a spy by an official of the Polish firm Polamco.

FBI Director Webster has said that the cases like Bell and Harper which come to public attention "are merely the tip of the iceberg." The counterintelligence information provided to the Select Committee confirms Judge Webster's statement.

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Although the Intelligence Committee does most of its work in closed hearings, we believe it is vital for the entire Senate and the public to be aware of the full dimensions of the espionage problem. For one thing, there is quite a bit that the average citizen can do to strengthen the nation's defenses, especially if the individual works for the federal government, a government contractor, or a high-tech industry or research program. The public also needs to know what we in government are doing about foreign espionage and whether we should be doing something more. For that reason, we plan to make a public report to the Senate at the end of the Select Committee's review of U.S. counterintelligence and security programs.

The subject of today's hearing is a significant element in the comprehensive review of U.S. counterintelligence and secruity programs that the Select Committee is conducting. This open hearing is therefore a good place to give your Subcommittee and the entire Senate a preliminary report on the Select Committee's work. Our report explains the context and importance of some specific recommendations we want to offer, based on the Select Committee's review of the hostile intelligence threat and U.S. countermeasures over the past several years.

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

From its inception, the Select Committee has given high priority to counterintelligence concerns. Two of the Committee's first legislative proposals -- the Foreign Intelligence Surveillance Act of 1978 and the Classified Information Procedures Act of 1980 -- have been a significant help to U.S. counterintelligence. Starting with FY 1979, the Intelligence Committee has reviewed the U.S. counterintelligence budget as a whole and taken the lead to increase money and manpower for counterintelligence in the FBI, the CIA, and the Defense Department. The Committee has also looked at the damage done by major espionage cases, some of the deficiencies in personnel and communications security, the value of techniques such as the polygraph, and measures to improve counterintelligence operations and analysis.

At the beginning of the 99th Congress, we decided that one of the Committee's most important tasks under our leadership should be to make an independent assessment of the counterintelligence and security requirements for dealing with Soviet espionage and other hostile intelligence threats. Although we made this decision before the Walker case, it was already clear that espionage arrests were on the increase and that hostile intelligence operations posed a growing problem for national security.

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Thus far this year, the Intelligence Committee has held at least seven closed sessions on counterintelligence and security matters. We have considered CI program and budget requirements for FY 1986, the need for greater control over the numbers and activities of hostile intelligence officers in this country, the security situation at the U.S. Embassy in Moscow, the damage done by the Walker espionage network, the requirements for a $35 million supplemental appropriation for security countermeasures at U.S. facilities abroad, and a comprehensive survey by senior FBI and CIA officials of the full extent of the hostile intelligence threat. Most recently, the Committee has had several briefings on the Howard case. We are reviewing the personnel, security, and management procedures associated with this case and other ramifications of the defection of senior KGB official Vitaly Yurchenko, who served in the Soviet Embassy here in 1975-80.

1. The Espionage Problem

The hostile intelligence threat has many facets, and not all of them surface in espionage prosecutions. It is important to consider all the dimensions in developing a national strategy to deal with that threat.

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

a. The Human Dimension

The Howard and Walker cases are the latest in a series of major espionage cases that show how vulnerable U.S. national security secrets are to foreign espionage. The expulsion of scores of Soviet agents from France and Britain, the penetrations of the West German Government, and other espionage cases in Norway and Greece indicate the worldwide success of Soviet intelligence operations. As documented in the recent interagency report on Soviet Acquisition of Militarily Significant Western Technology, the Soviets devote massive resources to systematic efforts to penetrate Western governments and high-tech industry.

The Soviets also use other East European intelligence services as surrogates, because they have access to places where Soviets cannot go. The Bell and Harper cases illustrated the effectivenesss of Polish intelligence in penetrating U.S. defense industries. In the Harper case, top Soviet intelligence officials came to Warsaw to get the information on U.S. missile defense systems. East German agents arrested in the United States over the past two years include a woman courier in an espionage network and a prominent scientist attempting to recruit American scientists.

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

At a closed hearing last July, the FBI told the Select Committee that the espionage cases of the last two years have involved billions of dollars of actual and potential damage to U.S. military programs. The problem is compounded by the vast number of Chinese officials and visitors in the U.S. While U.S.-PRC relations are good, there is clear evidence of clandestine intelligence operations by the Chinese in the United States. These activities greatly increase the burden on the FBI's counterintelligence resources.

An Intelligence Community study summarizes the human threat in the following terms:

> Despite the development of increasingly sophisticated technical means of intelligence collection, the human agent continues to be the most important key to satisfying a nation's intelligence needs. The Communist countries depend to a large degree on their human collection networks throughout the world to satisfy their U.S.-related intelligence requirements -- requirements ranging from acquisition of advanced technology, location and determination of the quality of strategic and conventional military forces, and assessment of U.S. reaction to international political incidents, to discovery of techniques used by U.S. counterintelligence. A major, highly structured effort is dedicated to the acquisition of U.S. cryptographic information and materials that would allow the exploitation of secure U.S. communications. Success in this area can fulfill many of the requirements mentioned above.

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

b. The Technical Threat

Electronic espionage is as serious as the human variety. The Soviets listen to our telecommunications from their diplomatic establishments, from ships off our shores, and from a sophisticated monitoring site at Lourdes, Cuba, that can intercept our domestic and international satellite communications channels. While the most sensitive data are encrypted, the Soviets can exploit uncoded communications that deal with sensitive military, scientific, and economic developments. If communications security is lax, they can also get classified data. In 1978, a Soviet diplomat defected to the United States and said that telephone and telex calls were monitored at the Soviet recreational facility in Glen Cove, New York, which required the shipment of tons of material to Moscow annually. Satellite communications are potentially an extremely valuable source of information as they can simultaneously transmit thousands of telephone, T.V., and computer-to-computer transactions. The explosion in computer networks and the electronic transfer of data adds another major area for Soviet exploitation.

Computers and office equipment are also vulnerable to the most sophisticated electronic penetration and eavesdropping techniques. The reported discovery of bugged typewriters

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

at our Moscow Embassy illustrates the Soviets' impressive technical surveillance capabilities. Part of the problem is physical security, because the Soviets should never have gotten access to Moscow Embassy equipment.

Technical and human threats are inextricably linked. When foreign nationals employed at our embassies abroad can get access to sensitive offices or equipment, the chances for bugging greatly increase. At the same time, foreign nationals working in our embassies can assess the weaknesses of American employees on behalf of hostile intelligence services for possible recruitment. Here in this country, the human vulnerabilities that produce a Howard, a Walker, a Harper, or a Bell can given the Soviets not only specific facts and documents, but also codes and access to computer data systems that multiply the damage enormously.

c. Seeking A Balanced Response

The Select Committee is seeking to identify, in concert with the Executive branch, those actions that can be taken to improve U.S. counterintelligence and security protections without departing from our nation's basic principles.

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

In espionage, as in terrorism, there is a risk of overreaction that sacrifices individual rights and the rule of law for the sake of security.

Protection of national security secrets is not easy in a free society. Total preoccupation with security -- to the exclusion of other values -- would undermine the constitutional principles that America stands for throughout the world. If we seek to copy the secret police methods of our adversaries, they will have won a great victory. If, however, we show that the United States can protect its security without sacrificing fundamental freedoms, the essential superiority of an open society will be vindicated.

As President Reagan said in a nationwide radio address on June 29, 1985:

> "[W]e can counter this hostile threat and still remain true to our values. We don't need to fight repression by becoming repressive ourselves.... But we need to put our cleverness and determination to work and we need to deal severely with those who betray our country. We should begin by realizing that spying is a fact of life and that all of us need to be better informed about the unchanging realities of the Soviet system.... There is no quick fix to this problem. Without hysteria or finger pointing, let us move calmly and deliberately together to protect freedom."

Some proposals offered in the name of security may even be counterproductive. Closing down channels for the open exchange of unclassified basic scientific research

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

could do immense damage to the system of free scientific inquiry that keeps America so far ahead of the Soviets. The recent interagency report on Soviet acquisition of Western technology warned that restricting access to unclassified scientific data "may also inhibit the United States' own national research effort." Similarly, rapid expansion of the use of lie detector tests without the most careful quality controls and training for polygraph examiners not only could harm employee morale by treating individuals unfairly, but also could create a false sense of security and prevent other steps necessary to ensure the reliability of people in sensitive jobs.

2. Select Committee Study

On June 11, 1985, the Select Committee announced that it would conduct a comprehensive review of the Soviet intelligence threat and U.S. counterintelligence and security programs, including an examination of the implications for national security of the Walker espionage case. From the outset, our guiding principle has been to cooperate with the Executive branch in this effort. We have worked closely with the National Security Council staff and the relevant agencies and departments, and we expect that the President will shortly select a senior official to represent the

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Administration at a series of closed hearings on all aspects of counterintelligence and security. The objective is to reach agreement with the Administration on a common agenda for immediate actions and long-range decisions.

The closed hearings we have scheduled for this fall are planned to provide an overview of Administration actions on counterintelligence and security, including recent decisions and topics under review. We expect to take a close look at technical counterintelligence and security, at the long-range plans and requirements for counterespionage into the 1990s, at personnel and information security policies, and at the relationships between counterespionage and foreign policy. Much of our attention is focused on the adoption and implementation of recommendations that have already been made by other bodies, including the proposals made on June 6, 1985, by the Chairman and Ranking Minority Member of the Permanent Subcommittee on Investigations after hearings on security clearance programs last spring.

In preparation for our hearings, the Committee staff has conducted over fifty interviews with government officials and outside experts across the full spectrum of intelligence, military, diplomatic, industrial, and security fields. The staff has also pulled together the record of legislative and administrative actions in recent years.

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Most important of all, the Committee is compiling the results of a series of important studies of counterintelligence and security matters that have been conducted within the Executive branch. We also await the completion of two significant studies that are currently underway. The first is the report of the DoD Security Review Commission, chaired by General Richard G. Stilwell, the former Deputy Under Secretary of Defense for Policy. The Stilwell Commission has been charged with the task of identifying any "systematic vulnerabilities or weaknesses" brought to light as a result of the Walker case and making recommendations for changes to correct those deficiencies. The second study will come from an interagency task force headed by the Director of the Information Security Oversight Office, Steven Garfinkel, which is developing recommendations for a systematic attack on the problems of overclassification and overdistribution of sensitive information.

Based on these and previous Executive branch studies, the Select Committee's own closed hearings, and our ongoing dialogue with Administration officials, we hope to reach agreement on specific administrative and legislative actions that will have the joint support of the President and the Select Committee.

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

The Select Committee is also reviewing its own security procedures and those of the Senate as a whole. In July, the Committee offered its services to other Senate offices as a focal point for security briefings and advice. The Committee has implemented new security measures internally and will work with the Sergeant at Arms and other appropriate officials to improve security for all of us in the Senate.

3. Administrative and Congressional Initiatives

We need to identify what has already been accomplished in order to decide what more needs to be done. Concern about Soviet espionage and the need to improve U.S. countermeasures is not new, even though greater public attention has focused on the problem this year. Recent Administration initiatives have included:

-- Establishment of a policy review structure under the National Security Council for counterintelligence requirements and a small Community Counterintelligence Staff drawn from the FBI, CIA, and DoD to prepare national assessments of the hostile intelligence services threat and U.S. countermeasures.

-- The Foreign Missions Act of 1982, which created a new Office of Foreign Missions in the State Department to exercise greater control over the activities of foreign officials in this country. Under the able leadership of its Director, former FBI counterintelligence official James E. Nolan, the Foreign Missions Office has used this authority to enhance U.S. security within the framework of diplomatic reciprocity.

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

-- NSDD-145 on telecommunications and automated information systems security, issued by the President in 1984 to promote the development of coherent, long-range plans for improving U.S. communications and computer security.

-- Defense Department actions this year to reduce the number of security clearances, to enforce need-to-know limits on access to particular programs or activities, to tighten procedures for granting clearances, and to require that supervisors evaluate the security performance and reliability of cleared personnel.

-- A Presidentially-ordered five-year buildup of FBI foreign counterintelligence resources, which began in 1983 and has had full Congressional support in the annual Intelligence Authorization Acts.

-- Substantial increases in funding for the counter-intelligence programs of the military services and DIA, whose budgets are consolidated in the DoD Foreign Counterintelligence Program managed by the office of the Deputy Under Secretary of Defense for Policy. These increases have also had full support in the Intelligence Authorization Acts.

These Administration actions have made progress, but as the President emphasized in his June 29 address, much more must be accomplished.

In several areas, Congressional action has been taken to encourage or facilitate specific countermeasures:

-- The Huddleston-Leahy amendment to the Intelligence Authorization Act for FY 1985 requires annual reports to the Intelligence and Foreign Relations Committees on steps taken to reduce the disparities in numbers and treatment between officials in the United States from countries that engage in hostile intelligence activities and U.S. officials in those countries.

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

-- The Leahy-Cohen amendment to the State Department Authorization Act for FY 1986 establishes the policy that the numbers of U.S. and Soviet embassy and consular personnel should be substantially equivalent, unless the President makes an exception, and requires that a plan to achieve equivalence be submitted by February, 1986.

-- The Roth amendment to the State Department Authorization Act for FY 1986 authorizes the State Department to regulate the activities of U.N. Secretariat personnel and requires that such personnel be subject to the same controls as diplomats from their home country, unless the requirement is waived by the Secretary of State.

-- The Durenberger-Leahy amendment to the FY 1985 Supplemental Appropriations Bill provides $35 million to enhance security countermeasures at U.S. Embassies and other facilities abroad.

-- The State Department Authorization Act for FY 1986 calls for replacing Soviet employees at our Moscow Embassy with Americans to the extent practicable.

-- The Statement of Managers accompanying the Conference Report on the State Department Authorization Act for FY 1986 calls for a report on illicit electronic surveillance in the United States by foreign governments.

In addition to these measures already enacted, the pending Conference Report on the Defense Department Authorization Act for FY 1986 includes provisions offered by Senator Nunn to add funds for reducing the security clearance backlog, to require Presidential guidance and a report on personnel security policy, and to give DoD background investigations a

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

conditional exemption from OPM regulations. The pending defense bill also contains a new article in the Uniform Code of Military Justice permitting the death penalty for espionage in certain circumstances, a requirement for a report on the desirability of reinstituting the death penalty for civilian espionage, and limits on the "test program" for expanded use of polygraph examiniations in DoD so as to ensure quality controls and prevent mistakes. The conference on the Intelligence Authorization Act for FY 1986 is considering Senate provisions to increase Defense Department access to to criminal records for employee security background checks and to facilitate military counterintelligence double agent operations, as well as a House proposal for a DCI report on security vulnerabilities abroad.

While individual Senators may have differing views on one or another of these actions, the record clearly demonstrates a vigorous and determined effort by the Congress to address serious problems.

4. A Strategic Approach to Counterintelligence and Security

This list of Administration and Congressional initiatives hardly scratches the surface of the numerous recommendations for counterintelligence and security improvements that

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

have been made by various recent studies, mainly within the Executive branch. The Select Committee has been reviewing these proposals with Administration officials so as to arrive at a common agenda. It is increasingly clear that a strategic framework is needed for deciding where to concentrate. Thus far, both the Administration and the Congress have addressed these issues piecemeal. Many different agencies and Congressional committees have taken up parts of the problem, but nowhere has anyone tried to pull all the elements together in one place for a comprehensive assessment.

Recognizing this vacuum, the Select Committee has begun exactly that kind of systematic review. The Select Committee has had the benefit of some of the best thinking in the government as we work with Administration officials to reach agreement on the essential elements of a national strategy.

a. A National Counterintelligence Strategy

We believe we are close to an agreement, based on statements of the President and our consultations with key NSC officials, that the Executive branch should develop a national counterintelligence strategy. We are making a distinction here between "counterintelligence" measures and "security" programs. The best way to explain the difference

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

is to say that counterintelligence measures deal directly with hostile intelligence service activities, while security programs are the indirect defensive measures that minimize vulnerabilities.

From this perspective, a national counterintelligence strategy is not limited to the FBI, CIA, and DoD agencies that carry the "counterintelligence" label. It also includes those diplomatic and regulatory policies that control the numbers and movements of hostile intelligence service officers in this country and at U.S. facilities abroad. Each year, in the formal classified justification for funds for its Foreign Counterintelligence Program, the FBI advises Congress that, even with increased resources, the FBI cannot cope with the hostile intelligence threat unless measures are also taken to reduce the number of potential intelligence officers in this country. Where the numbers cannot be reduced, controls on their movements can assist the FBI in making better use of limited resources.

The organizational structure is already in place to develop and implement a national counterintelligence strategy. The relevant NSC committees and the Community CI Staff can provide the necessary forum for policy development, planning, and oversight of implementation. The Presidential

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

mandate is also clear. In his address of June 29, the President said the Administration had "developed a list of things to be accomplished in the counterintelligence and security areas." He said he was "tasking Cabinet officers to implement the improvements and reforms... on a priority basis." The areas mentioned by the President were;

-- Better means for informing the public about the Soviet intelligence threat.

-- Reduction of the size of the hostile intelligence presence in the U.S. from the present level of more than 2,500 Soviet bloc officials.

-- Establishing "a balance between the size of the Soviet diplomatic presence in the United States and the U.S. presence in the Soviet Union."

-- Better controls on "foreign intelligence agents working at the U.N. who have utilized that organization as a spy nest."

-- Improvement of U.S. counterintelligence capabilities, including "better coordination between counterintelligence agencies, better analysis of hostile threats" and adequate legal authority.

The basic question is whether the Executive branch will implement these measures (and other, classified actions) in the face of opposition from elements that have a vested interest in leaving things the way they are. In some areas, legislation may be required to implement fully the President's national counterintelligence strategy. In other areas, bureaucratic inertia must be overcome. The

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Select Committee on Intelligence stands ready to help with both processes.

b. A National Strategic Security Program

On the security side, we are discussing with the Administration the desirability of formulating a National Strategic Security Program. The government today does not have a comprehensive and integrated security program to protect the information and activities that have the greatest strategic importance to the United States. Such a program would develop national policy direction and guidance and oversee policy implementation for:

- Personnel security
- Information security and classification
- Telecommunications, computer, and other technical security
- Physical security
- Industrial security
- Interrelationships among these elements
- Research and development efforts
- Security awareness requirements

To assist the National Security Council, there should be a structure for long-term planning and systematic analysis of all aspects of strategic security. It should be a focal point for the various overlapping forums that now divide responsibility for security policy.

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

This is not a new proposal. Almost thirty years ago, the Congress established a Commission on Government Security with members appointed by the President and the Congressional leadership. Its chairman was a former President of the American Bar Association, and the Vice Chairman was Senator John Stennis. In its 1957 report, the Commission called for a Central Security Office to ensure greater uniformity and higher quality for personnel and industrial security throughout the government. The Commission also stressed "the dangers to national security that arise out of overclassification of information which retards scientific and technological progress" -- and proposed abolishing the Confidential classification because the danger of access to such material was "not significant" and the clearance requirements afforded "no real security-clearance check." The passage of nearly thirty years has not diminished the relevance of these recommendations.

Among the options we expect to see emerge from the Stilwell Commission is an improved personnel security system for those positions with access to information or activities of the greatest strategic importance. We will need to consider more stringent requirements for such

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

positions, including regular financial reports; prior notice of all foreign travel; high personal reliability standards with enforcement by superiors; a clearance policy that selects the most qualified personnel, rather than merely weeding out the worst; and a strong inspection system. It may also be necessary to consider legislation to apply to such positions post-employment obligations and perhaps revised criminal penalties.

These are examples of specific ideas that are being considered as part of the agenda for immediate actions and long-term decisions to strengthen U.S. strategic security. In addition, when we proposed what became the $35 million FY 1985 supplemental appropriation for security countermeasures abroad, we asked the DCI to plan how to use those funds in the context of a long-range strategy for dealing with hostile intelligence threats to U.S. facilities overseas. There may well be merit in proposals to institute a "systems security budget" for telecommunications and information systems security in order to coordinate U.S. Government efforts to influence private industry to undertake the development and production of more secure equipment and systems. And a better balance is needed between high-cost research on technical security projects and the current

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

inadequate funding for research on personnel security. The most secure hardware and software are no guarantee against a Walker, a Bell, or a Harper who decides to sell out his country. When security countermeasures against Soviet espionage are assessed in a single forum, the significance of such gaps becomes clearer and innovative policy may result.

5. Recommendations to Limit the Hostile Intelligence Presence

The importance of limiting the hostile intelligence presence in the United States should be obvious to everyone. Nevertheless, foreign policy considerations and perhaps legal obstacles have inhibited the Executive branch for many years from taking reasonable steps to make it more difficult for hostile intelligence services to operate inside this country. Creating a less favorable environment for espionage operations inside the United States should be the foundation of a national strategy. While we are still considering various proposals for improving the capabilities of the FBI and other U.S. counterintelligence agencies and for improved security measures, four recommendations deserve immediate attention. Each is fully consistent with the President's stated goals and should be implemented by the Executive branch unless there are legal obstacles requiring new legislation.

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

a. Equivalence in U.S.-Soviet Embassy/Consular Personnel

The Leahy-Cohen amendment establishes a policy of, in the words of the President on June 29, requiring "a balance between the size of the Soviet diplomatic presence in the United States and the U.S. presence in the Soviet Union." Some State Department officials appear to believe that this balance should be achieved solely by increasing the number of Americans in Moscow, to replace Soviet nationals employed at our Embassy. This totally misreads the intent of Congress and conflicts with the President's policy. While replacing Soviet nationals with Americans in Moscow will help improve security at the Embassy, it need not be done wholesale. Equally, if not more important, is a gradual reduction in Soviet personnel in the United States, as the President made clear when he said "we need to reduce the size of the hostile intelligence threat we're up against in this country." In determining equivalence, it is vital to ensure that we count all the Soviets employed at their embassy and consulates, and not just those on the official diplomatic list.

b. Reducing the Size of the Soviet U.N. Mission

Besides Soviet embassy and consulate personnel, the

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

largest number of Soviet officials in the United States are assigned to the Soviet Mission to the United Nations (SMUN). That is the next place to cut in achieving the President's goal of making a significant reduction in the 2,500 Soviet bloc officials in this country. The SMUN is more than twice the size of any other country's U.N. mission -- the next largest being the U.S. and Chinese missions. It should be possible for the United States to insist on the principle of equivalence as the base-line for reaching agreement with the U.N. on the size of the SMUN. This reduction in the number of potential intelligence officers would make a significant difference as far as the FBI's counterintelligence burden in New York City is concerned. It is not hard to imagine the enormous difficulties that confront the FBI in covering the activities of possible intelligence officers in a place like Manhattan.

c. Foreign Missions Office Controls on Warsaw Pact Country Representatives

Although the State Department has restricted travel in the United States by Soviet officials, placing some areas off limits and requiring Soviet officials to make travel arrangements through the Foreign Missions Office, similar

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

controls have not been placed on officials of other Warsaw Pact countries. Yet there is overwhelming evidence that the Soviets use the intelligence services of Warsaw Pact countries as surrogates. The recent report on Soviet Acquisition of Militarily Significant Western Technology documents these relationships fully. It reflects the Intelligence Community's judgment that the Soviets are likely to intensify their efforts by "increasing their dependance on surrogates among the East European intelligence services." The report also notes that one of the reasons for the "considerable success" of East European services is that "they operate under less severe travel restrictions" than do the Soviets. Given the evidence of this growing threat, the State Department should at least require Warsaw Pact country representatives to make travel arrangements through the Office of Foreign Missions. Moreover, if the FBI detects officials or representatives of a Warsaw Pact nation engaging in espionage-related activities in a particular area of the country, such as Silicon Valley, that area should be placed off limits to that country.

East European governments do not always require that U.S. officials make travel arrangements through a central government office. Realistically, however, in that part of

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

the world the security police know about virtually every aspect of American official travel. In an open society like ours, the imposition of a requirement to make travel reservations through the Foreign Missions Office is surely consistent with the principle of reciprocity.

d. Regulation of Foreign-Controlled Commercial Entities

The Foreign Missions Act applies not only to diplomatic establishments such as embassies and U.N. missions, but also to state trading organizations and other entities that perform governmental functions. There is, once again, clear counterintelligence information establishing that Soviet and Warsaw Pact trading companies and other commercial entities in the U.S. controlled by those countries are engaged in espionage-related activities. There are two avenues to pursue in regulating their operations.

First, the Export Administration Act as adopted earlier this year authorizes the Commerce Department to require a license for transfer of controlled goods or technology to an embassy or other "affiliate" of a Communist government in the United States. This language should be applied by the Commerce Department to commercial entities that are owned or controlled by Communist governments and that may be used to transfer technology abroad surreptitiously.

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Second, the Foreign Missions Act requirements should be applied to these same entities. Under the law as it now stands, such requirements clearly can be applied to state trading organizations such as the Soviet company AMTORG. It is more difficult, however, to apply the Foreign Missions Act to other Soviet bloc-controlled businesses. To close this gap, legislation should be enacted to amend the Foreign Missions Act and authorize the State Department to apply its requirements to "affiliates" of foreign governments, with the same meaning as in the Export Administration Act. A bill for this purpose will be introduced shortly.

These four steps -- equalizing U.S. and Soviet embassy and consular personnel, reducing the size of the Soviet U.N. Mission, requiring Foreign Mission Office travel controls for Warsaw Pact country representatives, and regulating foreign-controlled commercial entities -- are necessary to implement a national counterintelligence strategy. These hearings before the Permanent Subcommittee on Investigations will perform a vital function by letting the American public and all elements of the Executive branch know why such measures are necessary and how strongly they are supported in the Congress.

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

STAT
Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0

Page Denied

Next 2 Page(s) In Document Denied

Sanitized Copy Approved for Release 2011/03/17 : CIA-RDP87B00858R000300440005-0